IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

Credit Card Fraud Detection using Recurrent Attributes

Navneet Jain[1], Vasima Khan[2]

UIT BU Computer Science Department, Barkatullah University, Bhopal, India[1-2]

Abstract: It is very important to extract the right features from transactional data in implementing a credit card fraud detection model. It is normally done by combining the transactions in order to observe the spending patterns of the customers. We propose to create a new set of features based on analyzing the periodic behavior of the time of a transaction using the von Mises distribution in this paper. We compare credit card fraud detection models, and evaluate how the different sets of features have an impact on the results with the help of a real credit card fraud dataset provided by a large European card processing company. The results show an average increase in savings of 13% by including the proposed periodic features into the methods. The methodology proposed in this paper is currently being incorporated into the fraud detection system of aforementioned card processing company.

Keywords: Cost sensitive learning; Fraud detection; von Mises distribution.

INTRODUCTION

Credit card fraud has been an increasing problem worldwide. Representing an increase of 14.8% compared with 2011 [1], the total level of fraud reached 1.33 billion Euros in the Single Euro Payments Area during 2012. Moreover, payments across non-traditional channels (mobile, internet,) accounted for 60% of the fraud, whereas it was 46% in 2008. This opens new challenges as new fraud patterns arise, and current fraud detection systems are less capable in preventing these frauds. Furthermore, to avoid being detected, fraudsters regularly change their strategies, something that makes traditional deceit recognition tools, such as expert rules, insufficient [2].

In fraud detection, the use of machine learning has been an interesting topic in recent years. Based on machine learning techniques, different detection systems have been successfully used for this problem, in particular: neural networks [3], Bayesian learning [4], artificial immune systems, hybrid models, support vector machines, peer group analysis, online learning and social network analysis.

Nowadays, enterprises and public institutions need automatic systems to implement fraud detection and have to face a growing presence of fraud initiatives. Since it is not always possible or easy for a human analyst to detect fraudulent patterns in transaction datasets, constantly characterized by a large number of samples, many dimensions and online updates, automatic systems are imperative. Also, the card holder is not reliable in reporting the theft, loss or fraudulent use of a card [5]. Since the number of fraudulent transactions is much smaller than the legitimate ones, the data allocation is unstable, i.e. skewed towards non-fraudulent inspections. Methods have been proposed to improve the performances of many learning algorithms which underperform when used for unbalanced dataset. Many other factors other than unbalancedness determine the difficulty of a classification/detection task. Another in influential factor is the amount of wholly coinciding of the classes of appeal due to limited information that transaction records provide about the nature of the process [6].

It is very important to use those features that allow precise classification when constructing a credit card fraud detection model. Raw transactional features, such as time, amount, and place of the transaction are only used by typical models. However, the spending behavior of the customer, which is expected to help discover fraud patterns [7], is not taken into account by these approaches. In [8], where Whitrow et al. proposed a transaction aggregation strategy in order to take into account a customer spending behaviour is a standard way to include these behavioural spending patterns? In classification of the transactions made during the last given number of hours, first by card or account number, then by transaction type, merchant group, country or other, followed by calculating the number of transactions or the total amount spent on those transactions, the computation of the aggregated features consists.

In many situations, the prediction of user behaviour in financial systems can be used. A lot of money and other resources can be saved by predicting client migration, marketing or public relations. The fraud of credit lines, especially credit card payments is one of the most interesting fields of prediction. A reduction of 2.5% of fraud triggers a saving of one million dollars per year [9] for the high data traffic of 400,000 transactions per day. Certainly, all transactions which deal with accounts of known misuse are not authorized. Experienced people can tell that the transactions are probably misused, caused by stolen cards or fake merchants even if they are formally valid. So, a credit card transaction before it is known as illegal, fraud has to be avoided.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

People can no longer control all increasing number of transactions. As solution one can put the experience of expert into an expert system. The experts knowledge, even when it
can be obtained clearly, changes regularly with new kinds of organized attacks and patterns of credit card fraud this is the disadvantage of this traditional approach. No predefined fraud models as in [10] but automatic learning algorithms are needed in order to keep track with this.

Along with an increasing volume of payment traffic, advancement and expansion of modern technology and sophistication of fraudulent tactics, credit card fraud is growing. Significant losses and great inconvenience to issuing companies, merchants and customers world-wide is caused by it. Entire card fraud dissipation on UK issued cards grew by 25% from the last year and total amount was 535 million (APACS, 2008) in year 2007. Within the following categories the range of fraud tactics observed in the industry can be broadly described: In response to practices of issuing companies and merchants to protect against identified tactics in the future this list evolves over time as fraudsters adapt new strategies like lost and stolen card fraud, counterfeit card fraud, card not present fraud, mail non-receipt card fraud, account takeover fraud and application fraud. Currently in the UK, Card-not-Present fraud, where the physical card is not present at the pointof-sale is the largest type of credit card fraud. As face-to-face fraudulent transactions become increasingly difficult, it is expected that the volume of CNP fraud will continue to grow.

A number of challenges for designing a fraud detection system are presented by the nature of transaction data and some particular operational issues:

- Each transaction contains more than 70 fields of coded information furthermore the number of transactions processed by credit card issuers daily is high. Transaction data is heterogeneous and changing time to time within and between accounts. For different groups of merchants, holiday seasons and geographical regions patterns and trends vary expressively.
- Within the credit card industry the generally accepted fraud rate is 0.10.2%, i.e. the occurrence of fraud is relatively rare. Repeatedly this leads to the problem that the majority of cases detected by the fraud detection system as being potentially fraudulent are in fact legal. This type of error is referred to as false positive (FP). The associated costs and customer inconvenience increased as the number of FPs increase.
- For further investigation, alerts emerging from the fraud detection system are usually passed on to the fraud department. For verification of the transactions, where it is required by the bank policy, the suspected cases are followed up with a call to a cardholder. As a result of this, the number of alerts should be kept at a level such that it can be handled by the available number of investigators and fraud analysts.
- When the cardholder identifies that their account has been compromised fraudulent cases missed by the fraud detection system are reported to the issuing company. Resulting in a delay in correctly labelling each case, this can take up to several months. Some fraudulent cases are mislabelled because they remain unidentified. Thus, a fraud detection model is almost certainly trained on noisy data.

Based on analyzing the time of a transaction, we propose a new set of features in this paper. At similar hours, it is expected from customer to make transactions. This is the logic behind it. Hence, based on the periodic behaviour of a transaction time, using the von Mises distribution [11] a new method for creating features is proposed. In particular, if the time of a new transaction is within the confidence interval of the previous transaction time new time features should estimate.

Furthermore, using two kinds of classification algorithms; cost-insensitive [12] and example-dependent cost-sensitive using a real credit card fraud dataset provided by a large European card company we compare various sets of features (raw, aggregated and periodic). By using the proposed periodic features the results show an average increase in the savings of 13%. Additionally, to implement a state-of-the-art fraud detection system that will help to combat fraud the outcome of this paper is being currently used once the implementation stage is finished.

The remainder of the paper is organized as follows. In Section 2, we discuss current approaches to create the features used in fraud detection models. We present our proposed methodology to create periodic features in section 3. Afterwards, the experimental setup and the results are given in Sections 4 and 5. Finally, conclusions and discussions of the paper are presented in Section 6.

LITERATUTRE SURVEY

V. Van Vlasselaer, C. Bravo, O. Caelen, T. EliassiRad(2015) APATE, a novel approach to detect fraudulent credit card transactions conducted in online stores. Our approach combines (1)intrinsic attributes obtained from the properties of incoming transactions history using the fundamentals of RFM (Recency Frequency Monetary); and (2) network-based features by utilizing the network of credit card beares and merchants and detecting a suspiciousness score for each network object. Our results show that both intrinsic and network-based attributes are two firmly interlace sides of the same picture. The collaboration of these two types of features leads to the best performing models which reach AUC-scores higher than 0.98.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

R. Brause, T. Langsdorf, and M. Hepp, The prevention of credit card fraud is an important application for prediction techniques. One major obstacle for using neural network training techniques is the high necessary diagnostic quality: Since only one financial transaction of a thousand is invalid no prediction success less than 99.9% is acceptable.

S. Panigrahi, A. Kundu, S. Sural, and A. Majumdar(2009) The fraud detection system(FDS) consists of four components, namely, rule-based filter, DempsterShafer adder, transaction history database and Bayesian learner. In the constraint-based part, we detect the speculation level of each incoming transaction based on the extent of its deviation from good pattern. DempsterShafers theory is used to combine various such proofs and an inceptive stance is computed. The transaction is classified as normal, abnormal or suspicious depending on this initial belief.

M. Krivko(2010) The framework for a hybrid model for plastic card fraud detection systems. The proposed data customized approach combines elements of supervised and unsupervised methodologies aiming to compensate for the individual deficiencies of the methods.

S. Bhattacharyya, S. Jha, K. Tharakunnel(2011) This paper evaluates two advanced data mining approaches, support vector machines and random forests, combined with the well known planning reversion, as part of an attempt to better detect (and thus control and prosecute) credit card fraud. The study is based on real-life data of transactions from an international credit card operation.

D. J. Weston, D. J. Hand, N. M. Adams(2008) Peer group analysis is an unsupervised method for monitoring behaviour over time. In the context of plastic card fraud detection, this technique can be used to find anomalous transactions. These are transactions that deviate strongly from their peer group and are flagged as potentially fraudulent. Time alignment, the quality of the peer groups and the timeliness of assigning fraud flags to transactions are described.

A. D. Pozzolo, O. Caelen, Y.-A. Le Borgne(2014) Some answers from the practitioners perspective by focusing on three crucial issues: unbalancedness, nonstationarity and assessment. The analysis is made possible by a real credit card dataset provided by our industrial partner.

C. Whitrow, D. J. Hand, P. Juszczak, D. J. Weston(2008) A framework for transaction aggregation is considered and its effectiveness is evaluated against transaction-level detection, using a variety of classification methods and a realistic costbased performance measure. These methods are applied in two case studies using real data. Transaction accumulation is formed to be advantageous in many but not all circumstances. Also, the length of the aggregation period has a large impact upon performance.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Problem Definition

When using the aggregated features, there is still some information that is not completely captured by those features. In particular we are interested in analysing the time of the transaction. The logic behind this, is that a customer is expected to make transactions at similar hours. The issue when dealing with the time of the transaction, specifically, when analysing a feature such as the mean of transactions time, is that it is easy to make the mistake of using the arithmetic mean. Indeed, the arithmetic mean is not a correct way to average time because, it does not take into account the periodic behaviour of the time feature. For example, the arithmetic mean of transaction time of four transactions made at 2:00, 3:00, 22:00 and 23:00 is 12:30, which is counter intuitive since no transaction was made close to that time.

B. Proposed System Architecture

In this paper a method is proposed to overcome the limitation by modelling the time of the transaction as a periodic variable,in particular using the von Mises distribution. The von Mises distribution, also known as the periodic normal distribution, is a distribution of a wrapped normal distributed variable across a circle.

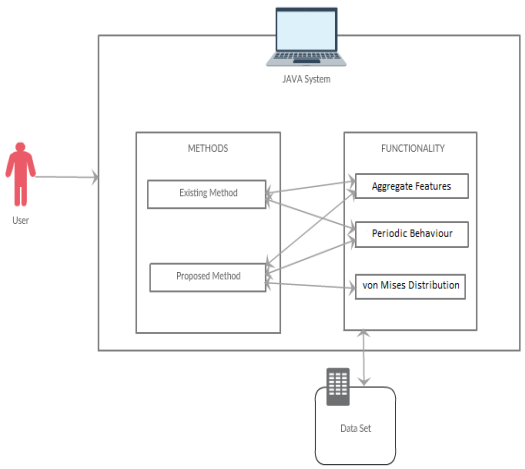

Fig. 1. System Architecture

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

IV. MATHEMATICAL MODEL

NP-Complete:

A decision problem is NP-complete if:

1) C is in NP, and
2) Every problem in NP is reducible to C in polynomial time.

C can be shown to be in NP by demonstrating that a candidate solution to C can be verified in polynomial time. Note that a problem satisfying condition 2 is said to be NP-hard, whether it satisfies condition 1. A consequence of this definition is that if we had a polynomial time algorithm (on a UTM, or any other Turing-equivalent abstract machine) for C, we could solve all problems in NP in polynomial time.

NP-Hard:

A decision problem H is NP-hard when for every problem L in NP, there is a polynomial-time reduction from L to H. An equivalent definition is to require that every problem Lin NP can be solved in polynomial time by an oracle machine with an oracle for H. Informally, we can think of an algorithm that can call such an oracle machine as a subroutine for solving H, and solves L in polynomial time, if the subroutine call takes only one step to compute. Another definition is to require that there is a polynomial-time reduction from an NP-complete problem G to H. As any problem L in NP reduces in polynomial time to G, Lreduces in turn to H in polynomial time so this new definition implies the previous one. It does not restrict the class NP-hard to decision problems, for instance it also includes search problems, or optimization problems.

- If P 6 ≠ NP, then NP-hard problems cannot be solved in polynomial time;
- If an optimization problem H has an NP-complete decision version L, then H is NP-hard

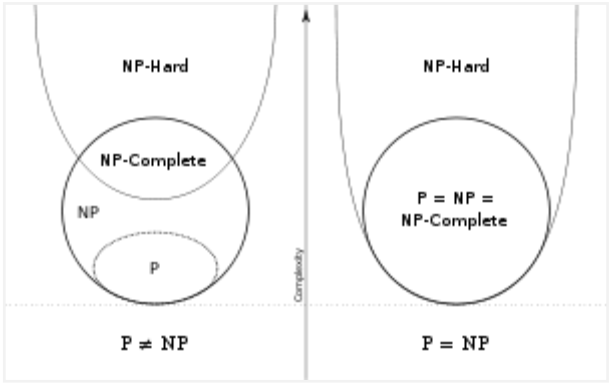

Fig. 2. NP-Hard and NP-Complete

V. EXPECTED RESULTS AND DISCUSSION

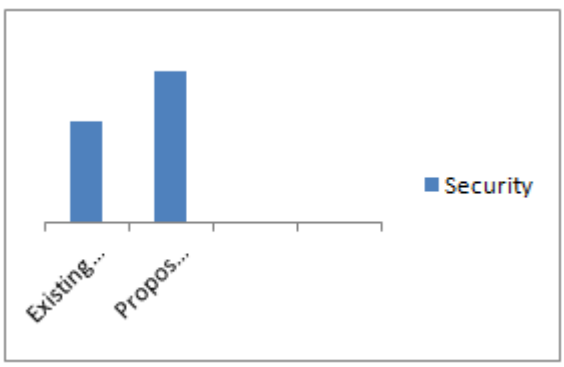

Fig. 3.

The Fig.3 shows graphical representation of security verses algorithms. Performance is estimated according to the security provided by algorithms. The Fig.4 shows graphical representation of time verses algorithms. Performance is estimated according to the time required for execution of algorithms.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

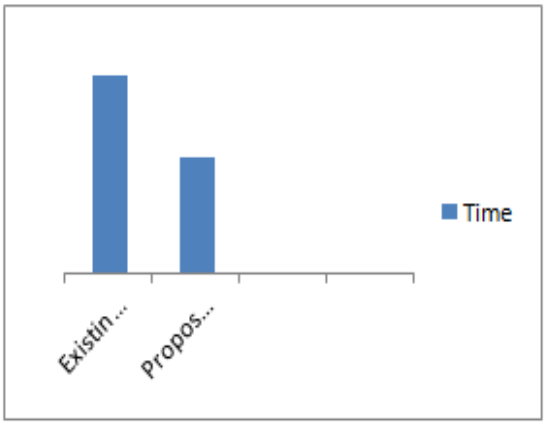

Fig. 4.

VI. CONCLUSION AND FUTURE WORK

In this paper we have shown the importance of using features that analyse the consumer behavior of individual card holders when constructing a credit card fraud detection model. We show that by preprocessing the data in order to include the recent consumer behaviour, the performance increases by more than 200% compared to using only the raw transaction information.

However, because this study was done using a dataset from a financial institution, we were not able to deeply discuss the specific features created, and the individual impact of each feature. Nevertheless, our framework is ample enough to be recreated with any kind of transactional data. Furthermore, when implementing this framework on a production fraud detection system, questions regarding response and calculation time of the different features should be addressed.

REFERENCES

[1] European Central Bank, Third report on card fraud, European Central Bank, Tech. Rep., 2014.
[2] V. Van Vlasselaer, C. Bravo, O. Caelen, T. Eliassi-Rad, L. Akoglu, M. Snoeck, and B. Baesens, APATE: A Novel Approach for Automated CreditCardTransactionFraudDetectionusingNetworkBasedExtensions, Decision Support Systems, vol. 75, pp. 3848, 2015.
[3] R. Brause, T. Langsdorf, and M. Hepp, Neural data mining for credit card fraud detection, Proceedings 11th International Conference on Tools with Articial Intelligence, pp. 103106, 1999.
[4] S. Panigrahi, A. Kundu, S. Sural, and A. Majumdar, Credit card fraud detection: A fusion approach using Dempster Shafer theory and Bayesian learning, Information Fusion, vol. 10, no. 4, pp. 354363, Oct. 2009.
[5] S. Bachmayer, Articial Immune Systems, Articial Immune Systems, vol. 5132, pp. 119131, 2008.
[6] M. Krivko, A hybrid model for plastic card fraud detection systems, Expert Systems with Applications, vol. 37, no. 8, pp. 60706076, Aug. 2010.
[7] S.Bhattacharyya,S.Jha,K.Tharakunnel,andJ.C.Westland,Datamining forcreditcardfraud:Acomparativestudy,DecisionSupportSystems,vol. 50, no. 3, pp. 602613, Feb. 2011.
[8] D. J. Weston, D. J. Hand, N. M. Adams, C. Whitrow, and P. Juszczak, Plastic card fraud detection using peer group analysis, Advances in Data Analysis and Classication, vol. 2, no. 1, pp. 4562, Mar. 2008.
[9] A. D. Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, Learned lessons in credit card fraud detection from a practitioner perspective, Expert Systems with Applications, vol. 41, no. 10, pp. 49154928, Aug. 2014.
[10] [C. Whitrow, D. J. Hand, P. Juszczak, D. J. Weston, and N. M. Adams, Transaction aggregation as a strategy for credit card fraud detection, Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 3055, Jul. 2008.
[11] N. I. Fisher, Statistical Analysis of Circular Data, 1996, vol. 9.
[12] C. M. Bishop, Pattern Recognition and Machine Learning, ser. Information science and statistics. Springer, 2006, vol. 4, no. 4.
[13] C. Elkan, The Foundations of Cost-Sensitive Learning, in Seventeenth International Joint Conference on Articial Intelligence, 2001, pp. 973978.
[14] R. Bolton and D. J. Hand, Unsupervised proling methods for fraud detection, in Credit Scoring and Credit Control VII, 2001.
[15] D. Tasoulis and N. Adams, Mining information from plastic card transaction streams, in Proceedings in 18th International Conference on Computational Statistics, 2008.
[16] S. Jha, M. Guillen, and J. Christopher Westland, Employing transaction aggregation strategy to detect credit card fraud, Expert Systems with Applications, vol. 39, no. 16, pp. 1265012657, 2012.
[17] A. Correa Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk, in 2013 12th International Conference on Machine Learning and Applications. Miami, USA: IEEE, Dec. 2013, pp. 333338.
[18] Improving Credit Card Fraud Detection with Calibrated Probabilities, in Proceedings of the fourteenth SIAM International Conference on Data Mining, Philadelphia, USA, 2014, pp. 677 685.
[19] R. J. Bolton, D. J. Hand, F. Provost, and L. Breiman, Statistical Fraud Detection: A Review, Statistical Science, vol. 17, no. 3, pp. 235255, 2002.
[20] D. J. Hand, C. Whitrow, N. M. Adams, P. Juszczak, and D. J. Weston, Performance criteria for plastic card fraud detection tools, Journal of the Operational Research Society, vol. 59, no. 7, pp. 956962, May 2007.
[21] A. Correa Bahnsen, D. Aouada, and B. Ottersten, ExampleDependent Cost-Sensitive Decision Trees, Expert Systems with Applications, vol. 42, no. 19, pp. 66096619, 2015.
[22] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, Scikit-learn: Machine learning in Python, Journal of Machine Learning Research, vol. 12, pp. 28252830, 2011.
[23] A. Correa Bahnsen, D. Aouada, and B. Ottersten, Example-Dependent Cost-Sensitive Logistic Regression for Credit Scoring, in 2014 13th International Conference on Machine Learning and Applications. Detroit, USA: IEEE, 2014, pp. 263269.